IT Professional Technical Services

SITE Program

T#:14ATM

Request for Offers (RFO)

For Technology Services

Issued By

MN Department of Human Services –Sex Offender Program

Project Title: Expansion of Phoenix System

Categories: **Web Application Design & Development (2)**

Analyst (1)

Note: Vendor must be approved in both categories and be able to provide the full team of resources in order to respond. Vendors who are unable to provide the full team of 3 resources will not be considered.

Business Need

The Minnesota Sex Offender Program (MSOP) is seeking to further enhance the existing browser-based software application, known as Phoenix. This project will add critical modules and make enhancements to Phoenix application. Phoenix was developed in 2010 to serve the business needs of the MSOP. Since then the system has evolved and become increasingly complex. Legislative requirements and changes to the program have necessitated further development and enhancements of Phoenix.

This project requires a Business Analyst and two C# (C-sharp) Software Developers.

Qualified candidates will work in an Agile environment. The respective job functions of the candidates include:
- Documenting as-is and to-be business process analysis,
- Documenting user stories,
- Creating activity, sequence, class, object and state diagrams as required to detail out the project requirements,
- Creating data dictionary and data mapping documents,
- Writing acceptance criteria, and test scenarios,
- Coordinating user acceptance testing,
- Conducting user training,
- Coordinating project activities with a team to document and improve business processes with complex rules,
- Complying with statutory and legal requirements,
- Attending HIPAA security awareness training.

The candidates will collaborate with other internal and external staff including technical team members, project manager, project sponsor, subject matter experts, and other Minnesota Information Technology Services (MN.IT) and Department of Human Services (DHS) staff as necessary.

Development of the Phoenix system enhances the productivity of the MSOP, provides workflows and allows for creation of data points eliminating the need for dual entries. The collective gathering of data in one central system provides easier and greater delivery of information to the staff and to the stakeholders while maintaining the integrity of the data. The proposed additional development and enhancement to the system will increase the data collection and administration of the database, providing easier management processes and support of the overall goals of the MSOP.

The following bullet points outline the components and modules that need to be delivered during the fiscal year 2016 ending in June 30, 2016.

- Communication Log
  The Communication Log features will allow all MSOP staff to provide comments and observations about clients. These observations need to be reported by location of occurrence. All users should be able to search the Communication Log for entries about clients using different filters and criteria. These entries are also subject to the retention schedule set by the Records Manager.

- Data Correction
  The ability to route a set of data (document) to a selected staff to amend data while preserving the original data in the database, and maintain data integrity between Phoenix and FileNet[*]. This feature should include automated narrative of what data was changed along with staff's electronic signature and an amended title.

- Conversion of Existing Word-based forms
  MSOP personnel use about two-dozen forms for assessing and interviewing clients. These forms were created as Word documents, which are inefficient and cumbersome to maintain. Users will need to re-enter the data from these Word-based documents into the Phoenix system. MSOP is asking to incorporate these forms into the Phoenix system directly so users can capture the needed data in one place. MSOP is also seeking to incorporate workflows behind these forms. This will allow staff to route the assessments to appropriate staff for necessary actions. Additionally, MSOP is requesting the vendor to create the building blocks for these forms so administrative staff can use templates to create additional forms and workflows when needed.

- Administrative Function to add Documents, and Create Form
  Develop the ability for authorized MSOP staff to create and edit forms as needed. This includes the ability to create reports for FileNet, capture data elements, signature workflow, review workflow, and edit format capability.

- Restrictions Status
  The ability to create reports for FileNet[*], capture data elements, signature workflow, review workflow, edit format capability, display restrictions on a user screen, and prompt user for required tasks.

- Client Admission Workflow
  This includes the ability to create work flow processes built into Phoenix that will send staff notices when they have tasks that are due, and collect information on when and what tasks are being performed, reports for FileNet[*], capture data elements, signature workflow, review workflow, edit format capability, and prompt user of required tasks.

- Enhancements such as but not limited to the following that will be prioritized and determined during the contract:
  - Entry of Multiple Legal Statuses
    Allow dual civil commits and display all active legal statuses on Individual Treatment Progress, Quarterly and Annual Treatment Reports, Personal Information page, and Legal Status History page. Update admission screens to accommodate this feature

  - Enhancements to HIPAA HiTech Audit Log
    Create records of actions taken by staff for purposes of review and audit

  - Forwarding an Incident Report

Ability to forward to a supervisor a returned report for completion when staff are no longer employed or out of the facility for an extended amount of time

- o Staff Notification of Follow up Ticket
  Notification to personnel when they have been assigned follow up incident reports

- o Refining Physical Clearance Screen
  Data entry screen for Physical Clearance needs additional items to match the policy

- o Client Availability Calendar
  Ability to click on a client's calendar and schedule a course or see whether a client is available

- o Reasonable Modification Plans/Notification
  An alert mechanism for reasonable modification so staff knows prior to printing or action that the modification exist (i.e. Large font modification, alert prior to printing client schedule)

- o Trip Slip for Site Change
  Create trip slips when site changes occur which will eliminate duplicate data entry

- o Restraint/Search Record
  Add data elements needed for statute requirement such as Reason for unclothed visual body search (UVBS); Additional staff involved in restraints; Yes/No for staff assisted UVBS; Location of UVBS. Reduce duplicate data entry between Phoenix and Incident Reports. Review the inclusion of 253B.03 Subd 1. (b) developmental disability exception. Add restraint types: Restraint Board, Restraint Gurney, and reason for Restraint Reduction.

- o Psycho-Ed Record Edits for Historical Data
  Change the facilitator field to either manually type in a or generate from organization's directory lookup

- o Signature Suffix Date Dependency
  When a suffix of staff is updated, that suffix is for signature moving forward. Past signature suffix needs to reflect this change

- o Admin review of Incident Report follow up tickets
  Ability to view and filters follow up tickets on screen

- o Ability to View Incomplete Incident Reports
  Ability for supervisors to view draft and returned incident reports to follow up with staff

Additional enhancements may be defined as the program evolves.

Project Deliverables

Followings are the required deliverables for this project.

Task	Deliverable
Current business process (as-is)	Narratives (diagrams if beneficial)
Future business process (to-be)	Narratives, user stories and diagrams
Business rules	Narratives
Requirement tracing	Any documents created during the discovery phase of the project

Security, and Role-Bases Access	Architectural diagrams and technical documentation
Screen mockups and wireframes	Design documents
Data conversion	Migration of current data to new data source where applicable
Work effort estimates	Any and all documents and communications pertinent to estimation effort
System Documentation	All technical, system and user manuals
User acceptance testing scripts	Step by step test scripts
System verification testing	Reports of test success/failure
Issues log	Documentation of issues identified during testing and how to fix them

The project team has adopted Agile software development menifesto. Each sprint is expected to be 4 weeks. Tasks will be assigned at the beginning of the sprint. Analysts will track their progress against assigned tasks using *Team Foundation Software*. The State may adjust the sprint duration depending on the needs of the program, in which case tasks will be adjusted accordingly.

Efforts within each sprint is estimated at 40 hours per week multiplied by 4 weeks for a total of 160 hours. The vendor may invoice at the end of each production release (deliverable) for services completed during the most recent period.

Project Milestones and Schedule

Milestone	Timeline
Project Start Date	11/11/2015
Schedule interview and discovery session with MSOP staff	12/07/2015
Validate process model and compile requirement for new components	12/30/2015
Creation of mockup screens and visuals	01/13/2016
Start development of the new modules	01/13/2016 (development of certain items can start while discovery sessions are taking place)
Test the new components	March – May 2016
Develop training models	May 2016
Deliver training	June 2016
Create and deliver documentation	Throughout the project
Install new modules and enhancements	June 2016
Post-installation support	June 2016, for period of one month after installing new modules
Project End Date**	June 30, 2017

Additional modules will be defined as the needs of the program evolves and other enhancements emerge due to changing policies and legislative process.

* *FileNet is the standard document repository system within DHS.*
** *Some items listed in this RFO need to be delivered before the end of fiscal year 2016 and the project will continue into state fiscal year 2017.*

Project Environment

- Phoenix is a browser-based software system developed using .NET class libraries and C# programming language, and it uses Active Directory for authentication and authorization. The development environment consists of virtual machines, virtual desktop infrastructure, Windows 2008, Visual Studio 2010 (moving to version 2013) and .Net framework 4.0.
- Phoenix has a user interface / presentation layer that requests functionality through the business logic layer (BLL), which interacts with data via the data access layer (DAL).
- Construction of Phoenix began in 2010 and the project team has added many complex modules over the years.
- The project team uses SharePoint for collaboration and for tracking of various project documentation. The team also uses *Balsamiq* prototyping tool for creating screen mock-ups.
- Team Foundation Server (TFS) version 2013 is used as a repository for source and other project artifacts. TFS is also used for branching code, for building deployable packages, for testing activities, and for documenting bugs and issues.

Project Requirements

The MSOP manages multiple sites and as such employees at these sites access Phoenix using laptop and desktop computers.

Once the new modules and features are developed, contractors will train MSOP staff on how to use the new features. These training sessions will accompany Wiki documentation pages that the contractor staff will create as part of the final product.

The contractor staff will comply with all the security, enterprise architect, role-based security model, and hardware and software maintenance requirements that DHS ITS and MN.IT have established.

The system will be subject to review by the MN.IT Enterprise Security Office including passing a Veracode scan at the VL4 assurance level.

IT Accessibility Standards

All documents and other work products delivered by the vendor must be accessible in order to conform with the State Accessibility Standard. Information about the Standard can be found at:
http://mn.gov/mnit/programs/policies/accessibility/.

Responsibilities Expected of the Selected Vendor

The selected contractor staff will:

- Define and document functional and business requirements,

- Conduct Business Process Modeling,

- Create new data models and re-design existing models where practicable,

- Create and update existing use case specifications,

- Create wireframes and mock-ups,

- Extend the existing role-based and security model to the new modules,

- Develop and update as-is and to-be process flow diagrams,

- Create and execute test plans and test scripts for all stages of testing,

- Discover, and manage business rules and create new rules,

- Reflect desired business practices in new or modified business rules,

- Understand how rules are enforced and impacted,, and how rules-related issues such as conflicting rules would be resolved,

- Validate business rules and develop corresponding scenarios for test scripts,

- Assist in project planning and development of project schedule,

- Develop new modules using tools and standards adopted by DHS ITS and MN.IT,

- Conduct training sessions on new modules and features,

- Develop automatic test scripts,

- Provide technical walkthrough sessions to project team members,

- Provide technical support on new software modules,

- Record software issues and provide resolutions,

- Communicate and correspond with business users,

- Work with the MN.IT project manager to effectively bring project to closure.

Required Skills (to be scored as pass/fail)

This project requires the following qualifications.

I. The vendor will provide an Analyst with the following required minimum skills:
- 5 years of experience eliciting and documenting business requirements,
- 5 years of experience performing various types of testing such as unit, functional, performance, capacity, stress, regression and end to end,
- 5 years of experience reporting on issues and conducting root cause analysis,
- 5 years of experience leading defect tracking and reporting,
- 5 years of experience producing test plans and test strategy,
- 5 years of experience creating manual and automated test scripts,
- 5 years of experience facilitating user acceptance testing,
- 5 engagements using agile methodology,
- 3 engagements constructing and running SQL command for troubleshooting and issue resolution purposes,
- 5 years of experience conducting gap analysis for documenting current and future states of business 3 engagements using SharePoint for document management,
- 5 engagements providing estimates on requests,
- 2 years of experience mapping requirements to the Web Content Accessibility Guidelines (WCAG 2.0),
- 2 years of experience with HIPAA and HITECH requirements.

II. The vendor will provide two (2) .NET C# Developers with the following required minimum skills
- 5 years of experience with Research, design, define, develop, test, document, and implement new software, system or change existing applications in keeping with organizational standards,
- 5 years of experience interpreting business requirements and specifications,
- 5 years of experience developing software according to written technical specifications,
- 3 engagements developing transactional and browser-based software using Microsoft Visual Studio versions 2013 and 2015, and Microsoft SQL Server database,
- 3 engagements creating, documenting, and implementing unit test plans, scripts, and test harnesses,
- 5 engagements producing architectural and technical documentation pertinent to project,
- 5 engagements providing estimates on requests,
- 5 engagements working with technical staff such as infrastructure, network, and server teams to resolve application related issues,
- 2 years of experience validating code with a variety of accessibility testing tools including WAVE and color contrast analyzers,
- 2 years of experience with secure coding principals such as: OWASP Top 10, SANS Top 25.

Desired Skills

- Experience working with government / State government,
- Experience working with Microsoft Active Directory,
- Experience working with Agile manifesto,
- Experience working with SharePoint,

Process Schedule

Deadline for Questions   4:00 p.m. on 10/22/2015
Anticipated Posted Response to Questions   4:00 p.m. on 10/28/2015
Proposals due   4:00 p.m. on 11/02/2015
Anticipated proposal evaluation begins   8:00 a.m. on 11/04/2015
Anticipated proposal evaluation & decision   4:00 p.m. on 11/06/2015

Questions

Any questions regarding this Request for Offers should be submitted via e-mail according to the date and time listed in the process schedule to:

      Name: Mehrdad Shabestari
      Organization: MN.IT
      Email Address: Mehrdad.Shabestari@state.mn.us

Questions and answers will be posted via an addendum to the RFO on the Office of MN.IT Services website (http://mn.gov/buyit/14atm/rfo/active.html) according to the process schedule above.

Other persons ARE NOT authorized to discuss this RFO or its requirements with anyone throughout the selection process and responders should not rely on information obtained from non-authorized individuals. If it is discovered a Responder contacted other State staff other than the individual above, the responder's proposal may be removed from further consideration.

The STATE reserves the right to determine if further information is needed to better understand the information presented. This may include a request for a presentation.

RFO Evaluation Process

- Required skills – pass/fail
- Desired skills - 70%
- Cost - 30%

This Request for Offers does not obligate the state to award a work order or complete the assignment, and the state reserves the right to cancel the solicitation if it is considered to be in its best interest. The Organization reserves the right to reject any and all proposals.

Submission Format

The proposal should be assembled as follows:

1. **Cover Page**

      Vendor Name
      Vendor Address
      Vendor City, State, Zip
      Contact Name for Vendor
      Contact's direct phone/cell phone (if applicable)
      Contact's email
      Resource Name being submitted

Hourly Rates

2. **Overall Experience:**

   1. Provide narrative, including companies and contacts where your resource has demonstrated the required skills as previously noted. If pass/fail requirements are not met, the State will discontinue further scoring of the proposal.

   2. Points will be awarded based on the desired skills noted above. Provide one paragraph which highlights the resource's desired skills noted above.

   3. Attach a resume(s) for proposed resource(s) in addition to the narrative description. Be certain the resume has dates of work and notes whether the resource was an employee or consultant.

   4. Also include the name of two references who can speak to the resources work on a similar project. Include the company name and address, reference name, reference email, reference phone number and a brief description of the project this resource completed.

3. Cost Proposal must be in a separate document and not listed any other place in your submission. Document naming convention: <Company Name><Resource Name><Category> Cost Proposal. Example ABC Company, John Doe, Analyst Cost Proposal.

4. Conflict of interest statement as it relates to this project
   Responder must complete the conflict of interest statement as it relates to this project in accordance with the requirements set forth below.

5. Additional Statement and forms:
   required forms to be returned or additional provisions that must be included in proposal.

   a. Affirmative Action Certificate of Compliance (if over $100,000, including extension options)
      http://www.mmd.admin.state.mn.us/doc/affaction.doc

   b. Equal Pay Certificate Form (if proposals exceeds $500,000, including extension options)
      http://www.mmd.admin.state.mn.us/doc/equalpaycertificate.doc

   c. Affidavit of non-collusion
      http://www.mmd.admin.state.mn.us/doc/noncollusion-2.doc

   d. Certification Regarding Lobbying (if over $100,000, including extension options)
      http://www.mmd.admin.state.mn.us/doc/lobbying.doc

Proposal Submission Instructions

Vendors may only submit one response to the RFO with one resume per resource. Vendors who cannot provide the full team of resources will not be considered.

- Response Information:
  - Mehrdad Shabestari
  - Email only to mehrdad.shabestari@state.mn.us
  - Subject line: RFO – Phoenix Project

- Submissions are due according to the schedule listed in this document.
- **A copy of the response must also be sent to MNIT.SITE@state.mn.us for vendor performance tracking.**
- **You must submit an email with your response or email notification that you will not respond to MNIT.SITE@state.mn.us. Failure to do either of these tasks will count against your program activity and may result in removal from the program.**

General Requirements

Proposal Contents

By submission of a proposal, Responder warrants that the information provided is true, correct and reliable for purposes of evaluation for potential award of this work order. The submission of inaccurate or misleading information may be grounds for disqualification from the award as well as subject the responder to suspension or debarment proceedings as well as other remedies available by law.

Liability

In the performance of this contract by Contractor, or Contractor's agents or employees, the contractor must indemnify, save, and hold harmless the State, its agents, and employees, from any claims or causes of action, including attorney's fees incurred by the state, to the extent caused by Contractor's:

1) Intentional, willful, or negligent acts or omissions; or
2) Actions that give rise to strict liability; or
3) Breach of contract or warranty.

The indemnification obligations of this section do not apply in the event the claim or cause of action is the result of the State's sole negligence. This clause will not be construed to bar any legal remedies the Contractor may have for the State's failure to fulfill its obligation under this contract.

Disposition of Responses

All materials submitted in response to this RFO will become property of the State and will become public record in accordance with Minnesota Statutes, section 13.591, after the evaluation process is completed. Pursuant to the statute, completion of the evaluation process occurs when the government entity has completed negotiating the contract with the selected vendor. If the Responder submits information in response to this RFO that it believes to be trade secret materials, as defined by the Minnesota Government Data Practices Act, Minn. Stat. § 13.37, the Responder must: clearly mark all trade secret materials in its response at the time the response is submitted, include a statement with its response justifying the trade secret designation for each item, and defend any action seeking release of the materials it believes to be trade secret, and indemnify and hold harmless the State, its agents and employees, from any judgments or damages awarded against the State in favor of the party requesting the materials, and any and all costs connected with that defense. This indemnification survives the State's award of a contract. In submitting a response to this RFO, the Responder agrees that this indemnification survives as long as the trade secret materials are in possession of the State.

The State will not consider the prices submitted by the Responder to be proprietary or trade secret materials.

Conflicts of Interest

Responder must provide a list of all entities with which it has relationships that create, or appear to create, a conflict of interest with the work that is contemplated in this request for proposals. The list should indicate the name of the entity, the relationship, and a discussion of the conflict.

The responder warrants that, to the best of its knowledge and belief, and except as otherwise disclosed, there are no relevant facts or circumstances which could give rise to organizational conflicts of interest. An organizational conflict of interest exists when, because of existing or planned activities or because of relationships with other persons, a vendor is unable or potentially unable to render impartial assistance or advice to the State, or the vendor's objectivity in performing the contract work is or might be otherwise impaired, or the vendor has an unfair competitive advantage. The responder agrees that, if after award, an organizational conflict of interest is discovered, an immediate and full disclosure in writing must be made to the Assistant Director of the Department of Administration's Materials Management Division ("MMD") which must include a description of the action which the contractor has taken or proposes to take to avoid or mitigate such conflicts. If an organization conflict of interest is determined to exist, the State may, at its discretion, cancel the contract. In the event the responder was aware of an organizational conflict of interest prior to the award of the contract and did not disclose the conflict to MMD, the State may terminate the contract for default. The provisions of this clause must be

included in all subcontracts for work to be performed similar to the service provided by the prime contractor, and the terms "contract," "contractor," and "contracting officer" modified appropriately to preserve the State's rights.

IT Accessibility Standards

All documents and other work products delivered by the vendor must be accessible in order to conform with the State Accessibility Standard. Information about the Standard can be found at: **http://mn.gov/mnit/programs/policies/accessibility/**.

Preference to Targeted Group and Economically Disadvantaged Business and Individuals

In accordance with Minnesota Rules, part 1230.1810, subpart B and Minnesota Rules, part 1230.1830, certified Targeted Group Businesses and individuals submitting proposals as prime contractors will receive a six percent preference in the evaluation of their proposal, and certified Economically Disadvantaged Businesses and individuals submitting proposals as prime contractors will receive a six percent preference in the evaluation of their proposal. Eligible TG businesses must be currently certified by the Materials Management Division prior to the solicitation opening date and time. For information regarding certification, contact the Materials Management Helpline at 651.296.2600, or you may reach the Helpline by email at mmdhelp.line@state.mn.us. For TTY/TDD communications, contact the Helpline through the Minnesota Relay Services at 1.800.627.3529.

Veteran-Owned Preference

In accordance with Minn. Stat. § 16C.16, subd. 6a, (a) Except when mandated by the federal government as a condition of receiving federal funds, the commissioner shall award up to a six percent preference on state procurement to **certified small businesses** that are **majority-owned and operated by veterans.**

In accordance with Minn. Stat. § 16C.19 (d), a veteran-owned small business, the principal place of business of which is in Minnesota, is certified if it has been verified by the United States Department of Veterans Affairs as being either a veteran-owned small business or a service disabled veteran-owned small business, in accordance with Public Law 109-461 and Code of Federal Regulations, title 38, part 74.

To receive a preference the veteran-owned small business must meet the statutory requirements above by the solicitation opening date and time.

If you are claiming the veteran-owned preference, **attach documentation, sign and return the Veteran-Owned Preference Form with your response to the solicitation.** Only eligible veteran-owned small businesses that meet the statutory requirements and provide adequate documentation will be given the preference.

Foreign Outsourcing of Work Prohibited

All services under this contract shall be performed within the borders of the United States. All storage and processing of information shall be performed within the borders of the United States. This provision also applies to work performed by subcontractors at all tiers.

Work Force Certification

For all contracts estimated to be in excess of $100,000, responders are required to complete the Affirmative Action Certificate of Compliance and return it with the response. As required by Minnesota Rule 5000.3600, "It is hereby agreed between the parties that Minnesota Statute § 363A.36 and Minnesota Rule 5000.3400 - 5000.3600 are incorporated into any contract between these parties based upon this specification or any modification of it. A copy of Minnesota Statute § 363A.36 and Minnesota Rule 5000.3400 - 5000.3600 are available upon request from the contracting agency."

Equal Pay Certification

If the Response to this solicitation could be in excess of $500,000, the Responder must obtain an Equal Pay Certificate from the Minnesota Department of Human Rights (MDHR) or claim an exemption prior to contract execution. A responder

is exempt if it has not employed more than 40 full-time employees on any single working day in one state during the previous 12 months. Please contact MDHR with questions at: 651-539-1095 (metro), 1-800-657-3704 (toll free), 711 or 1-800-627-3529 (MN Relay) or at compliance.MDHR@state.mn.us.

Data Privacy and Security Terms

Responder will be required to agree to the following terms and conditions regarding the protection of private information.

"The CONTRACTOR and STATE must comply with the Minnesota Government Data Practices Act, Minn. Stat., ch. 13, and the Health Insurance Portability Accountability Act ["HIPAA"], 45 C.F.R. § 164.103, et seq., as it applies to all data provided by the STATE under this contract, and as it applies to all data created, collected, received, stored, used, maintained, or disseminated by the CONTRACTOR under this contract. The civil remedies of Minn. Stat. § 13.08 apply to the release of the data governed by the Minnesota Government Practices Act, Minn. Stat. ch. 13, by either the CONTRACTOR or the STATE. Additionally, the remedies of HIPAA apply to the release of data governed by that Act.

If the CONTRACTOR receives a request to release the data referred to in this clause, the CONTRACTOR must immediately notify and consult with the STATE's Authorized Representative as to how the CONTRACTOR should respond to the request. The CONTRACTOR's response to the request shall comply with applicable law.

1.Information Covered by this Provision. In carrying out its duties, CONTRACTOR shall be handling one or more types of private information, collectively referred to as "protected information," concerning individual clients of STATE programs or services. "Protected information," for purposes of this contract, includes any or all of the following:

(a) Private data (as defined in Minn. Stat. §13.02, subd. 12), confidential data (as defined in Minn. Stat. §13.02, subd. 3), welfare data (as governed by Minn. Stat. §13.46), medical data (as governed by Minn. Stat. §13.384), and other non-public data governed elsewhere in the Minnesota Government Data Practices Act (MGDPA), Minn. Stats. Chapter 13;

(b) Health records (as governed by the Minnesota Health Records Act [Minn. Stat. §144.291 - 144.298]);

(c) Chemical health records (as governed by 42 U.S.C. § 290dd-2 and 42 C.F.R. § 2.1 to §2.67);

(d) Protected health information ("PHI") (as defined in and governed by the Health Insurance Portability Accountability Act ["HIPAA"], 45 C.F.R. § 160.103);

(e) Federal tax information ("FTI") (as protected by 26 U.S.C. 6103), and

(f) Other data subject to applicable state and federal statutes, rules, and regulations affecting the collection, storage, use, or dissemination of private or confidential information.

2 General Oversight Responsibilities. CONTRACTOR shall be responsible for ensuring proper handling and safeguarding by its employees, subcontractors, and authorized agents of protected information collected, created, used, maintained, or disclosed on behalf of STATE. This responsibility includes:

(a) Training: Ensuring that employees and agents comply with and are properly trained regarding, as applicable, the laws listed in 7.1 and

(b) Minimum necessary access to information. CONTRACTOR shall comply with the "minimum necessary" access and disclosure rule set forth in the HIPAA and the MGDPA. The collection, creation, use, maintenance, and disclosure by CONTRACTOR shall be limited to "that necessary for the administration and management of programs specifically authorized by the legislature or local governing body or mandated by the federal government." *See*, *respectively*, 45 C.F.R. §§ 164.502(b) and 164.514(d), and Minn. Stat § 13.05 subd. 3.

(c) Information Requests. Unless provided for otherwise in this contract, if CONTRACTOR receives a request to release protected information, CONTRACTOR must immediately notify STATE. STATE shall provide CONTRACTOR instructions or direction concerning the release of the data to the requesting party before the data is released. See paragraph 7.3(e) below regarding requests from individuals for their own data.

3 Additional Duties to Ensure Proper Handling of Protected Information. The CONTRACTOR shall:

(a) Not use or disclose protected health information other than as permitted or required by this contract or as required by law;

(b) Use appropriate safeguards, and comply with Subpart C of 45 C.F.R. Part 164 with respect to electronic protected health information, to prevent use or disclosure of protected health information other than as provided for by this contract;

(c) As required at 45 C.F.R. §164.410, report to STATE any use or disclosure of protected health information that is not provided for by the contract of which CONTRACTOR becomes aware, including any breach of unsecured protected health information or any other "privacy" or "security incident" as described below. Upon direction from STATE, CONTRACTOR must also attempt to mitigate harmful effects resulting from the disclosure.

(i) For purposes of this contract, "Security incident" means the attempted or successful unauthorized access, use, disclosure, modification, or destruction of information or interference with system operations in an information system. Security incident shall not include pings and other broadcast attacks on CONTRACTOR's firewall, port scans, unsuccessful log-on attempts, denials of service, and any combination of the above; so long as such incidents do not result in unauthorized access, use or disclosure of STATE's information. "Privacy incident" means violation of the MGDPA and/or the HIPAA Privacy Rule (45 CFR Part 164, Subpart E), including, but not limited to, improper and/or unauthorized use or disclosure of protected information, and incidents in which the confidentiality of the information maintained by it has been breached.

(ii) The report to the STATE must be in writing and must be sent to STATE not more than seven (7) days after learning of such non-permitted use or disclosure. The report must, at a minimum: 1) Identify the nature of the non-permitted use or disclosure; 2) Identify the PHI used or disclosed; 3) Identify who made the non-permitted use or disclosure, and who received the non-permitted or violating disclosure, if known; 4) Identify what corrective action was taken or will be taken to prevent further non-permitted uses or disclosures; 5) Identify what was done or will be done to mitigate any deleterious effect of the non-permitted use or disclosure; and 6) Provide such other information, including any written documentation, as STATE may reasonably request.

(iii) CONTRACTOR will provide notice required by 45 C.F.R. §§ 164.404 through 164.408 to affected individuals, news media, and/or the Office of Civil Rights, Department of Health and Human Services, only upon direction from and in coordination with the STATE.

(d) In accordance with 45 C.F.R. §§ 164.502(e)(1)(ii) and 164.308(b)(2), if applicable, ensure that any subcontractors that create, receive, maintain, or transmit protected health information on behalf of the business associate agree in writing to the same restrictions, conditions, and requirements that apply to the business associate with respect to such information;

(e) Within ten (10) business days of a request from an individual or their designee, make available protected health information in a designated record set, consistent with Minn. Stat. § 13.04, subd. 3, and 45 C.F.R.§ 164.524;

(f) Within ten (10) business days, forward any request to make any amendment(s) to protected health information in a designated record set to STATE in order for the STATE to satisfy STATE's obligations under Minn. Stat. § 13.04, subd. 3 and 45 C.F.R. §164.526;

(g) Maintain and make available no later than fifteen (15) days after receipt of request from the STATE, the information required to provide an accounting of disclosures to the STATE as necessary to satisfy the STATE's obligations under 45 C.F.R. §164.528, or upon request from STATE respond directly to individual's request for an accounting of disclosures;

(h) To the extent the business associate is to carry out one or more of the STATE's obligation(s) under Subpart E of 45 C.F.R. Part 164, comply with the requirements of Subpart E that apply to the STATE in the performance of such obligation(s); and

(i) Make its internal practices, books, and records available to the Secretary for purposes of determining compliance with the HIPAA Rules.

(j) Business associate may not use or disclose protected health information in a manner that would violate Subpart E of 45 C.F.R. Part 164 if done by STATE.

4 STATE's Duties. STATE shall:

(a) Only release information which it is authorized by law or regulation to share with CONTRACTOR.

(b) Obtain any required consents, authorizations or other permissions that may be necessary for it to share information with CONTRACTOR.

(c) Notify CONTRACTOR of limitation(s), restrictions, changes, or revocation of permission by an individual to use or disclose protected information, to the extent that such limitation(s), restrictions, changes or revocation may affect CONTRACTOR'S use or permitted disclosure of protected information.

(d) Not request CONTRACTOR to use or disclose protected information in any manner that would not be permitted under law if done by STATE.

5 Disposition and/or Retention of Protected Information/Data upon Completion, Expiration, or Contract Termination. Upon completion, expiration, or termination of this contract, CONTRACTOR shall return to STATE or destroy all protected information received or created on behalf of STATE for purposes associated with this contract. CONTRACTOR shall return the protected information to the STATE's Authorized Representative *or* provide the state with written certification of destruction of the protected information. CONTRACTOR shall retain no copies of such protected information, provided that if both parties agree that such return or destruction is not feasible, or if CONTRACTOR is required by the applicable regulation, rule or statutory retention schedule to retain beyond the life of this contract, CONTRACTOR shall extend the protections of this contract to the protected information and refrain from further use or disclosure of such information, except for those purposes that make return or destruction infeasible, for as long as CONTRACTOR maintains the information.

6 Sanctions. In addition to acknowledging and accepting the general terms set forth in this contract relating to indemnification, the parties acknowledge that violation of the laws and protections described above could result in limitations being placed on future access to protected information, in investigation and imposition of sanctions (including but limited to civil and criminal penalties) by, among other agencies, the U.S. Department of Health and Human Services, Office for Civil Rights; the federal Internal Revenue Service (IRS); the Centers for Medicare & Medicaid Services (CMS); and the Office of the Attorney General for the State Minnesota.

7 Miscellaneous

(a) DHS Information Security Policy*.* Additional information regarding the handling and, as appropriate, destruction (upon expiration or termination of a contract or agreement) of protected information obtained from DHS is available at https://edocs.dhs.state.mn.us/lfserver/Public/DHS-4683-ENG.

(b) Effect of statutory amendments or rule changes. The Parties agree to take such action as is necessary to amend this contract from time to time as is necessary for compliance with the requirements of the laws listed in paragraph 7.1 of this clause or in any other applicable law.   However, any requirement in this contract or in the DHS Information Security Policy that is based upon HIPAA Rules or upon other federal or state information privacy or security laws means the requirement as it is *currently* in effect, including any applicable amendment(s), regardless of whether the contract has been amended to reflect the amendments(s).

(c) Interpretation. Any ambiguity in this contract shall be interpreted to permit compliance with the laws listed in paragraph 7.1 of this clause or in any other applicable law.

(d) Survival. The obligations of CONTRACTOR under this clause shall survive the termination of this contract.